Data protection and privacy in global networks

Louveaux, Sophie; Pérez Asinari, María Veroníca; Poullet, Yves

Published in:
The EDI Law Review

Publication date:
2001

Document Version
Publisher's PDF, also known as Version of record

Data Protection and Privacy in Global Networks: A European Approach . . .

*Meda Conference, Athens, 25 April 2001**

YVES POULLET, SOPHIE LOUVEAUX
AND MARÍA VERÓNICA PÉREZ ASINARI
Centre de Recherches Informatique et Droit, CRID-FUNDP, University of Namur, Belgium
(E-mail: yves.poullet@fundp.ac.be; sophie.louveaux@fundp.ac.be; veronica.perez@fundp.ac.be)

Abstract

This article will develop, in the first section, an approach based on a recent draft directive and focus on the interactions between the protection of privacy and the electronic communications sector, taking into account the developments of new services offered by this sector. In the second section, we analyse the delicate subject of transborder data flows, considering recent decisions taken in the European Union. Both aspects represent, in our opinion, the main issues that the European Union must face in the context of global networks as regards personal data protection.

Introductory Remarks

The Information Society is a challenge, a tool that provides us with innumerable benefits, nevertheless it requires the safeguarding of a certain way of life and values considered important for a society.[1] This idea could be considered as common place, but it is impossible to avoid. Information technologies can improve our quality of life.[2] They are an increasing power and, as such, need to be controlled to foster the democracy system and constitutional guarantees, and to stress liabilities.[3] The extraordinary growth of the Internet[4] has to be analysed from a legal point of view to prevent unbalanced situations.

Global networks represent a source of economic, social and cultural development, and at the same time, they have qualities[5] that have to be assessed in the light of the individuals right to privacy. Qualities that have been described as having 'capacity of voyeurism'.[6] The Internet has four characteristics that explain the reason why there are now open debates concerning privacy within its framework[7]: firstly, it is interactive and the use of the services offered by Internet multiplies therefore nominative data created by the data subject itself; secondly, the Internet is an open network that means that its use

*This article has been written in the context of the ECLIP Project (www.eclip.org) launched by the E.C. Commission in the context of the 5th Framework Programme (IST-1999-12278).

could create the problem of confidentiality by possible access of third persons to communications exchanged through this way but this point means also that due to global protocols like http or html, as an Internet user, one always has the possibility of switching from one web site to another web site, leaving at each time traces about now one uses the Internet ; thirdly, it is a global resource that multiplies transborder data flows and creates the fear of data paradises where no data protection can be ensured; finally, the Internet has a hidden face insofar as technologies like cookies, invisible hyperlinks or distance surveillance might be used for settling up invisible processings[8] which might be at the detriment of the data subject ... like cybermarketing, employee surveillance, etc.

This situation led Member States to start passing legislation to protect their citizens' fundamental right to privacy. Within the scope of the European Community this legislation was analysed from the perspective of the internal market, concluding that it could represent a barrier.[9]

This was one of the aims of both the General Data Protection Directive 95/46/EC[10] and particularly the Data Protection and Privacy in the Telecommunications Sector Directive 97/66/EC[11] based on *ex*-Article 7 A of the European Union Treaty (presently Article 14).

Technology progress[12] determines the urgent legal adaptation[13] of these directives in order to protect persons against new threats. The Internet, in that perspective, is definitively a 'test-bench' for the protection of privacy.[14] In other terms, data protection is more and more viewed by public and private policy makers as a fundamental precondition for the development of e-commerce.[15] This fundamental need of the potential and present Internet users for the protection of their data has also been underlined by different surveys operated in Europe and the US.[16]

This is the main purpose of the proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.[17] Recital 7 of the proposal proclaims

> Legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the electronic communications sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.[18]

Moreover, due to the fact that the Internet, but more generally all telecommunications networks are offered on a worldwide basis, the European Union must take into account the global character of these networks. As it has been revealed by the recent Echelon case,[19] a number of privacy threats

against data covered and protected by European Union directives might occur in cyberspace by data responsibles located outside Europe. It would be nonsense to restrict European Union protection to European borders. To take an example, more than 60 percent of the web sites are located in the US It is thus crucial to envisage the protection of European Internet users surfing on web sites located in the US. Certain of the general Data Protection Directive are facing this problem but the interpretation of these provisions is not easy. The European Union in that context has taken recent decisions. Their analysis might be of great interest beyond the specific cases envisaged.

To summarise the purposes of this article, they are twofold: the first chapter will be dedicated to an analysis of the provisions of a draft directive on electronic communication privacy. The second chapter will be devoted to the European approach of the increasing phenomena of transborder data flows. Both aspects represent the main issues that the European Union must face in order to ensure an effective protection of the European citizen.

1. 'Telecoms and Privacy': Towards a New Legal Framework

1.1. *Introduction*

The European Commission launched a review of the current telecommunications framework in 1999.[20] The goals of the review were fivefold: to promote more effective competition; to react to technological and market developments; to remove unnecessary regulation and to simplify associated administrative procedures; to strengthen the internal market; and to protect consumers.

The proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector is one of the consequences of this review. The present state of the enactment procedure might be described as follows: the proposed directive has been discussed by the European Parliament (Committee on Citizens' Freedoms and Rights, Justice and Home Affairs) on 11 July 2001. Certain amendments have been proposed notably as regards public directories and unsolicited communications (in favour of an opt out system). The present provisions on the processing of traffic and location data have also been challenged. In both cases, the Committee proposed a more liberal approach. The vote in plenary session is expected in September. On the contrary, the debate is not yet closed on that point, the Telecommunication Council of Ministers maintained, in its 27 June 2001 meeting, the European Commission point of view as regards the opt-in system for unsolicited commercial communications. We will refer to these present debates** in the following paragraphs.

**The article has been updated until the 1st of September.

The proposed directive aims at adapting Directive 97/66/EC[21] concerning the processing of personal data and the protection of privacy in the telecommunications sector to new technology, mainly to Internet related questions as regards privacy matters. Article 1.1 of the proposal describes:

> This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

Furthermore by broadening its scope of application and adopting a technology neutral terminology, the proposal aims at going beyond Internet related privacy issues and to impose to the electronic communications services the same rules as those applied in the off-line world:

> Directive 97/66/Ec should be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used.[22]

The following section aims at analysing the proposed modifications and their possible impact on electronic commerce activities.

1.2. *Analysis of the Draft Directive*

1.2.1. *Object and Scope*

Article 3 of the proposal defines the services concerned:

> This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the Community.

This article remains unchanged apart from the reference to 'electronic communication services' rather than to 'telecommunications services'. This broader term enables the directive to be adapted to developments in markets and technologies for electronic communications services. The term is intended to be technology-neutral. It is important however to specify that the present directive already applies to the Internet[23] so this is not as radical a change as one might think.

The deletion of the reference to ISDN and digital mobile networks can also be attributed to the idea of a technology neutral directive.

The proposal does not contain a definition of 'electronic communication services'. Nevertheless this definition can be found in the proposal of directive establishing a common framework for electronic communications services and networks[24]:

> 'electronic communications service' means services provided for remuneration which consist wholly or mainly in the transmission and routing of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.[25]

The scope of the directive is therefore limited to the provision of communications services 'for remuneration'. Does this imply that Internet access providers who provide a free access to the Internet do not fall within the scope of the directive?

It could be upheld that the remuneration does not necessarily have to be paid by Internet users, but can be paid by a third party such as an advertiser and therefore indirectly by the recipient of the service.[26] In the case of free access to the Internet, it is those who place banners or advertisements on the Internet pages whom in fact pay remuneration to Internet providers. Remuneration is given, and the specific directive therefore applies.[27] If this were not the case, the implications would be worrying. Indeed, very often it is the access providers offering free access to the Internet who infringe the data protection rules by either selling personal data to third parties (marketing companies, for example) or by processing the data for other purposes than those for which the data was initially collected. Albeit under the scope of application of General Directive 95/46 as concerns the protection of personal data and therefore subject to data protection rules provided in this directive, it is regrettable that they should be excluded from the stricter rules provided by the telecommunications specific directive. A clear indication as to the inclusion of free service providers should be provided in the directive.

The scope of protection excludes *'services providing, or exercising editorial control over content transmitted using electronic communications networks and services'*. This implies that hosting providers are included in the scope of the directive only if they merely host the content without exercising any control whatsoever over such content. The directive will however apply to a broad range of services like the provision of routers and interconnecting lines; the hosting of web sites; telecom networks operators services and the provision of Internet access. The definition offers the advantage of a clear separation between regulation of content and mere transmission[28] and reflects a similar distinction made in the Electronic Commerce Directive.[29] In practice, however,

it will be less easy to apply such a separation: an Internet service provider that also provides content by hosting its own site, will have to apply the General Directive to all its activities and the specific directive when providing mere access. Definitively, the solution enacted by the directive pleads clearly for an organisational clear separation between these two kinds of activities (that submitted to the directive and the other, not submitted), that might offer an efficient protection for data subjects.

The scope is limited to 'electronic communications services available to the public'.[30] Personal data processing for closed/private networks is excluded from the scope of the directive and therefore falls solely under the scope of Directive 95/46. This is regrettable and leads to a double regime for companies that have, for example, an Intranet and also use the Internet and other public electronic communication transmission services. The provisions of the proposed directive will not be able to be invoked by an employee against his employer in the event of an illicit use of traffic data. Article 29 Data Protection Working Party criticises this decision because private networks are gaining increasing importance in every day life and communications of citizens[31] and because a clear borderline between these two kinds of networks is difficult to determine.

Provisions are applicable for the protection of legitimate interests of subscribers who are legal persons.[32] This is not the case of Directive 95/46/EC, which only protects physical persons. But this was already the case with Directive 97/66/EC even if the proposed directive introduces, to the contrary or the previous one, certain provisions which are available only for physical persons. Some national laws, for instance Austria and Italy, have included the protection to legal persons while transposing Directive 95/46/EC.

1.2.2. *Security Principle*

This principle is proclaimed in Article 4 of the proposal:

> The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with respect to network security. Having regard to the state of the art and cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.[33]

Technology has a fundamental role in the protection of privacy problems since law is not self-acting.[34] In this respect Article 4 of the proposal imposes the obligation of providers to develop adequate technical and organisational measures for the protection of personal data. This obligation is similar to the obligation provided in Article 17 of Directive 95/46.

This provision must however be read in conjunction with Article 14 of the proposal. Indeed, Article 14 paragraph 1 of the proposal regulates the obligation of Member States to avoid imposing mandatory requirements for

specific technical features on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States. Although this paragraph does not deal with purely privacy matters but with internal market matters, it reflects the same techno-legal approach as can be found in Article 4. Even though the proposal imposes the adoption of security measures, Member States must ensure that these measures in no way impede the free circulation of equipment in and between Member States.

If the free market is the principle, however, the third paragraph of Article 14 stipulates clearly that if necessary the Commission would have to impose security measures as regards the terminal equipment components in order to ensure that the necessary privacy safeguards are incorporated. This provision is a direct application of the Directive on Terminal Equipment (1999/5/EC) which prescribes a certain number of essential requirements to be respected by the functioning of the terminal equipment. Privacy is one of these essential requirements for which the Commission might take certain measures as defining technical norms and imposing them. It follows the recommendation on 'Invisible and automatic processing of personal data on the Internet performed by software and hardware' issued by the 'Working party on the protection of individuals with regards to the processing of personal data on 23 February 1999,[35] which deals with phenomena like cookies, invisible identifiers and hyperlinks.

The second paragraph of Article 4 of the Proposal mandates providers to inform subscribers in case of residual security risks.[36] Since most users are unaware of the risks existing in the Internet, the obligation to inform must be exercised in a very active way.

1.2.3. *Confidentiality of Communications Principle*

This principle is the main pillar over which the protection of privacy in the communications sector can be built.[37] The proposal regulates it in Article 5, as follows:

> Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data, by persons other than users, without the consent of the users concerned, except when legally authorised to do so, in accordance with Article 15.1.[38]

Whereas Article 5 of Directive 97/66/EC on confidentiality referred to the content of the communication, the new proposal extends the protection to traffic-related data. The equal protection to content and traffic related data offers the advantage of not having to make a distinction between these two

concepts, a distinction which is often difficult and pointless to make. Indeed, when browsing on the Internet, the navigation data of an Internet user (URLs of sites visited) can reveal a great deal about the content of the communication taking place and should therefore be afforded a similar level of protection as the actual content. Indeed, the knowledge of the sites visited very often give a fairly accurate picture of the content of the communication.

Article 5 provides for three exceptions to the confidentiality of communications: with the consent of the users, when legally authorised to do so and '*any legally authorised recording of communications and the related traffic data in the course of lawful business practise for the purpose of providing evidence of a commercial transaction or of any other business communication*'.[39]

The reference to the consent of users implies the consent of all the parties to the communication. The distinction between a subscriber and a user must be reminded. Indeed the user 'means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to the service'.[4] Typically the distinction can be made in a workplace environment between the employee (user) and the employer (subscriber).[41]

The second exception to the confidentiality of communications is when legally authorised to do so in accordance with Article 15 (1) which provides that these exceptions must be adopted by the Member States by a legislative measure and must be necessary to '*safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system*'.[42] This provision reflects the European Convention of Human Rights which provides for specific guarantees to the exceptions to the fundamental human rights such as the right to privacy.[43] It also frames with the Council of Europe draft convention on cyber-crime,[44] which provides that a State may adopt legislative measures to empower its competent authorities to compel a service provider, within its existing technical capability to collect or record content data in real-time.

Finally, an exception to the principle of confidentiality is provided in paragraph 2 of Article 5:

> Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Article 29 of the Data Protection Working Party has expressed its opinion for deleting this paragraph of Article 5 by considering it too vague and thus allowing exemptions to confidentiality without respecting the basic conditions.[45] One can indeed question the legality of such a provision in the eyes

of the European Convention on Human Rights and of Article 15.1 of the present proposal. Furthermore, if the 'business practice' is 'lawful' in accordance with the general and the particular directives on data protection, there should be no need for providing a specific exemption.

1.2.4. *Traffic Data*

According to Article 6:

> Traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by the provider of a public communications network or service must be erased or made anonymous upon completion of the transmission, without prejudice to the provisions of paragraph 2, 3 and 4.

Traffic data are those data needed by the protocols to carry out the proper transmission from the sender to the recipient. Traffic data consist partly of information supplied by the sender (e.g. e-mail address of the recipient) and partly of technical information generated automatically during the processing of the e-mail (e.g. date and time sent, type and version of 'e-mail client').[46]

In accordance with the whole proposal design, the proposed article extends its coverage to all types of transmissions of electronic communications and replaces the terms 'upon termination of the call' by 'upon completion of the transmission'. This modification facilitates the consistent application of data protection principles on the Internet. Processing of header information, data such as the session login data or the list of websites visited by an Internet user must be considered as traffic data.[47]

Paragraph 2 declares that data which are necessary for the purposes of subscriber billing and interconnection payment may be processed up to the end of the period during which the bill may be lawfully challenged or payment pursued. This time limit will vary according to the legislation applicable in different Member States. It is therefore regrettable that a clear time limit has not been established in the provision itself. Furthermore the trend towards flat rate or free of charge access to communications services will mean that service providers will no longer be allowed to preserve traffic data.

The subscriber has to give his consent if the provider of a publicly available electronic communications service wants to process his/her traffic data for the purpose of marketing its own electronic communications services or for the provision of value added services (paragraph 3). The service provider must inform the subscriber of the types of traffic data, which are processed for the purposes mentioned above, and the duration for which this is done (§4).

As regards paragraph 3, a distinction must be made between the processing of traffic and billing data for the marketing of the providers *own* services or for the provision of value-added services. Whereas the processing of such data may only be processed for the marketing of the provider's own services,

processing may be authorised by the data subject for the processing of any value added service whether this service be provided by the initial provider or not. It is not altogether clear what the terms of value added services include. Considering the implications of this article, the term should be clarified in view of guaranteeing the limitation of the purpose.[48]

Another point to consider is that paragraph 1 refers to 'traffic data relating to subscribers and users'. However when paragraph 3 creates the exception mentioned above it only requires the consent of the subscriber. Considering that this is an exception it seems that it would be logical to include the 'user consent' as well when dealing with personal data.

According to paragraph 5, the processing of traffic data in accordance with Article 6, must be restricted to persons acting under the authority of providers of the public communications networks and services handling billing or traffic management, customer enquiries, fraud detection, marketing of the provider's own electronic communications services or providing a value-added service, and must be restricted to what is strictly necessary for the purposes of such activities. This latter phrase is a reminder of Article 6 of Directive 95/46 as concerns the quality of data. As for the persons who may process the data, the scope is so broad that one may question whether the article in effect restricts the persons who may process the data.

Finally paragraph 6 provides that Article 6 will apply without prejudice to the possibility for the competent authorities to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnections or billing disputes. This provision would notably enable the retention of traffic data for the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system and fits into line with the Council of Europe Convention on Cyber-crime,[49] which provides that a Member State may adopt legislative measures to empower its competent authorities to compel a service provider, within its existing technical capability to collect or record traffic data in real-time. At the Telecommunications Council meeting on 27 June 2001, Member States agreed to add a sentence on the retention of the traffic data in Recital 10:

> This directive does not affect the ability of the Member States to carry out lawful interception of electronic communications or to take measures, where necessary and justified, such as providing for the retention of traffic or location data for a limited period if it is necessary for any other purposes and in accordance with the general principles of Community law.

This clear reference to a possible legal duty of the services' providers to store traffic or location data in the context of their mandatory co-operation with law enforcement agencies creates a great risk since these providers might be tempted to use the data files normally to be used only in the context of public security

for other purposes and it will be difficult to detect this kind of illegitimate use.

1.2.5. *Presentation and Restriction of Calling and Connected Line Identification*

Article 8 remains unchanged. It regulates the right of anonymity of the caller, by having the right to prevent the presentation of the calling-line identification on a per-call basis, and also protect the called subscriber by giving him/her the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

1.2.6. *Location Data*

The proposal introduces a new provision giving privacy safeguards for subscribers and users with regard to mobile location[50] information services. Article 9 states:

> Where electronic communications networks are capable of processing location data other than traffic data, relating to users or subscribers of their services, these data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the added value service.

Before analysing the regulation itself the question of interpretation must be explained. The co-ordinating conjunction 'or' creates a delicate question when the 'user' cannot be identified with the 'subscriber'. One of the most frequent cases is that of the employee who has a mobile terminal and services contracted by his employer. Will it be necessary to inform both the employer and the employee to obtain double consent? Will the user who has given consent be able to temporarily deactivate the terminal localisation in every hypothesis or just under the provisions of the labour contract?[51]

We are dealing with a very sensitive aspect as it can affect a person's physical safety. That is why extremely careful measures should be taken. The location of a person could not only provoke discrimination by deducing aspects of the personality (red light districts, gambling places, etc.) but also attempt against physical safety if used for criminal purposes (kidnapping, robbery, etc.).[52]

The second paragraph of Article 9 establishes:

> Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of

charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

The Article 29 Working Party has criticised this regulation considering that the rule should be the opposite: the subscriber must have the possibility, via simple means, to freely allow the processing of location data for each delivery of an added-value service.[53]

Paragraph 3 provides for two further restrictions:

> processing of location data in accordance with paragraph 1 and 2 must be restricted to the persons acting under the authority of the provider of the electronic communications service or of third party providing added value service and must be restricted to what is necessary for the purposes of providing the value added service'.

1.2.7. *Directories of Subscribers*

According to Article 12.1., subscribers[54] must be informed, free of charge, about the purposes of a printed or electronic directory service in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. In addition paragraph 2 grants the subscribers the right to determine whether their personal data can be included in public directories and if so to which extent the data is relevant for the purpose of the directory as described by the provider.[55] They are also granted the right to verify, correct or withdraw such data.

This requirement has been welcomed by Article 29 Working Group.[56] Indeed it addresses a new service such as reverse searches in directories. These services enable, for example, to find out by means of a telephone number the name and address of a given person or the telephone numbers of persons living in the same street by means of the name of the street. Further usage can also be made of data appearing in a telephone directory by linking it to other data such as location data. Given that these purposes are not compatible with the initial purpose of including the data in a public directory and given the huge privacy implications that such applications can have, the specific consent of the subscriber should be given as regards these new purposes. In this respect the proposal does not go far enough since it only requires that the subscriber give its consent as to whether the data can be included in a public directory. A subscriber may indeed consent to the inclusion of the data in a public directory for the initial purpose of a directory which is to attribute a telephone number to a given person, this does not imply that the subscriber consents to further use of his data in reverse search applications. That issue has been recently evoked by the Committee on Citizen's Freedom and Rights of the European Parliament. If prior consent of the subscriber is not required for the inclusion of data in a public directory, consent will however be necessary as regards other functionalities than a simple search of communications details about another subscriber.

1.2.8. *Unsolicited Communications*

Directive 97/66/CE regulates the use of automated calling systems and fax machines for the purposes of direct marketing, which are only allowed in respect of subscribers who have given their prior consent.[57] This article is not updated with the increasing problem of 'spamming'.

'Spamming' is the practice of sending unsolicited e-mails or SMS messages, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has had no previous contact, and whose e-mail or mobile phone address was found in a public space on the Internet, such as a news group, mailing list, directory or website.[58]

It is an invasive practice because the collection of these addresses is made without the consent of the subject, who receives large amounts of unwanted communications and has to pay the cost of connection time.[59]

The present proposal includes 'electronic mail[60] for the purpose of direct marketing' under its regulation, and only allows it if the prior consent of the subscriber has been obtained.[61]

Neither the proposal nor Directive 95/46 define the term of direct marketing. A definition can be found in a Council of Europe recommendation and reads as follows:

> Direct marketing comprises all activities which make it possible to offer goods or services or to transmit any other messages to a segment of the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto.[62]

The term is therefore extremely wide and covers a number of activities whether commercial or not (political or fund-raising campaigns could be covered by the term, for example).

This change is not only the consequence of the legal adaptation to new technologies, but also an answer to the different regulations in the Member States as concerns spamming, which would affect the internal market. Five Member States[63] have already regulated the matter by considering it unlawful to send unsolicited commercial communications. Some other countries have adopted an opt-out system.

> Companies in opt-out countries may target e-mail addresses not only within their own country but as well to consumers in Member States with an opt-in system. Moreover, since e-mail addresses very often give no indication of the country of residence of the recipients, a system of divergent regimes within the internal market does not provide a common solution for the protection of consumer's privacy.'[64]

In this respect, the adoption of an opt-in regime can only be welcomed. As already said, the opt-in system has been challenged by the Committee of the

European Parliament in charge of the analysis of the proposed Directive and the issue is still being debated before the Council of Ministers. In particular, the opponents are arguing that this opt-in system would be contrary to previous provisions existing in other directives, namely the e-commerce Directive and the Distance Selling Directive, which are in favour of an opt-out system.

Having said this, a number of questions remain as concerns spamming and the implementation of an opt-in regime. Indeed, unless there has been prior contact (through the visit of a web site, for example) the obtaining of the data subject's consent to the sending of electronic mail presupposes the sending of a message in order to obtain this consent.[65] How can such a message be sent without itself being qualified as an unsolicited commercial communication?[66] Furthermore, if one respects the definition of the data subject's consent as given in Article 1 of Directive 95/46, the consent must be 'informed, specific and freely given'.[67] This prior message must therefore contain information namely as to the purposes for which the data is being processed and the possibility of opting out. Other questions must be answered: Who will be in charge of the opt-in list? How to ensure their quality, their interoperability and their liability? Can one consider that a consent might cover the commercial communications coming from different sectors?

More generally, the legitimacy of spamming with regard to the terms of Directive 95/46 can be questioned. Indeed Article 6 of this directive requires that personal data be collected for 'legitimate purposes'. This very idea of legitimacy implies the respect of proportionality between the interests of the data controller and the right to privacy of the data subject.[68] Applied within the context of spamming, one may question whether the interests of the data controller in sending a commercial communication can be said to override the burden of the cost of the data subject in receiving such a communication not only as concerns the costs of the transmission, but also the intrusiveness of such a technique as concerns a person's right to privacy.

As regards the sending of unsolicited commercial communications for the purposes of direct marketing by means other than automated calling systems, fax machines and electronic mail,[69] paragraph 2 of Article 12 leaves the choice up to the Member States between an opt-in regime ('*consent of the subscribers concerned*') or of opt-out ('*in respect of the subscribers who do not wish to receive these communications*').

According to this Article, paragraph 1 and 2 will only be applicable to natural persons. However, the proposal provides that Member States should also ensure that the legitimate interests of subscribers other than natural persons are sufficiently protected with regard to unsolicited communications. Can one consider that an opt-out system quite efficient will provide in any case sufficient protection?

2. Transborder Data Flows[70]

The Internet as a global network does not recognise frontiers. It is easy to send information abroad that contains personal data. Directive 95/46/EC has created as regards international transborder data flows (TBDF) either a liberalised area *ad intra* the European Community and strong obstacles *ad extra*. Within the EC territory even if certain disparities still exist and will not disappear in the future due to the various national ways of implementing the directive, the principle is the free flow of the data enacted by the article one of the Data Protection Directive, provided that the harmonisation of legislation is more or less achieved through the provisions of the directive.[71]

This is not the case outside the EC. There are countries with a high level of protection, countries with a totally different methodology of protection and countries with no protection of privacy as a fundamental right.

There is an increasing number of transborder data flows and we might identify among them different main categories:

- the first is definitively the use of the various Internet services insofar as most of the websites are located in North America and insofar as most of the Internet traffic is circulating through US infrastructures even if the communication relates only to European end users. As regards this use, as previously said, we might distinguish two kinds of flows generated by the use of the Internet: the first generated by a conscious action of the Internet user who might decide to have a look at certain pages, to use e-mail services and to make searches through search engines; the second is what we have called the invisible processing generated by certain operators outside of a deliberate decision of the Internet users;
- the second is more classic: it concerns data relating to a certain number of persons (customers or prospective customers) which are transferred to another company located in another country so that the latter might use this data essentially for marketing purposes;
- the third is the case where the exportation is due to the fact that the processing of data in that foreign country will reduce the costs;
- the fourth is also quite frequent: within a multinational company, the sending of data concerning employees or customers might be decided for the efficient management of the international consortium;
- lastly, we might imagine a final case where the transborder data flow is generated by the performance of a contract (like a flight reservation for tourist purpose) or by the accomplishment of an administrative duty (an investigation by law enforcement agencies) vis à vis specific people.

Different provisions of the European Data Protection Directive 95/46/EC are facing this diversity of situations. Our first concern will be to identify the hierarchy between these different provisions in order to delineate which provision is available for each specific category of transborder data flows

(2.1.). Having done that, we will then analyse the two main provisions of the Data Protection Directive and their interpretation and application: in Articles 25 (2.2.) and 26 (2.3.).

2.1. *The Hierarchy between the Different Provisions*

The Data Protection Directive contains three provisions which might be of application in case of transborder data flows: the first are definitively Articles 25 and 26 of the European Directive which are precisely dealing with the problem of transborder data flows. The main purpose of these two articles can be described as follows: the efforts put into place to afford a high level of protection for European citizens would be useless if through transferring data to third countries offering no guarantees the data subject remains finally without protection. So, Article 25.1 provides that transfers of personal data might take place only if the recipient's country offers 'adequate' protection. If it is not the case, the transborder data flows must be forbidden by Member States. Exceptionally the TBDF might be authorised in two cases enacted by Article 26. Article 26.1 describes certain types of transborder data flows where due to the circumstances of the flow or the peculiar end purpose of it, permission is granted. Article 26.2 provides another derogation: the data controller might adduce adequate safeguards notably by the use of contractual clauses with the recipient of data located in a country outside the European Union.

So the general principles as regards transborder data flows might be summarised as follows:

1. No transborder data flows can be authorised if the recipient's country is not ensuring an adequate level of protection;
2. By way of derogation to this general principle, transborder data flows might be authorised in two categories of cases, the first are listed in Article 26.1; the second ones provided by Article 26.2 require that a contract ensures the appropriate safeguards.

This very simple scheme is questioned by the need to take into consideration a third article of the Data Protection Directive also applicable as regards transborder data flows. Article 4.1 (c) stipulates that Member State legislation implementing the provisions of the Data Protection Directive has to be applied when the data controller established outside the European Union 'makes use of equipment situated on the territory of the Member State.'

Due to the vagueness of the expression 'make use of the equipment',[72] it is difficult to determine the real scope of these provisions when we consider the case of an Internet user accessing US website: can one decide that Article 25 is applicable provided that the visit represents a transborder data flow between an Internet user and a US data controller or might one on the contrary decide

that Article 4.1 (c) is applicable insofar as the data controller located outside of EU is using equipment situated on the territory of the said Member State? The consequence of the choice between these two articles is important: with the first option, the only point to take into consideration is the adequate protection offered by the US data controller or the possibility to apply one of the main exceptions foreseen by Article 26 (e.g. the sending of data was necessary for the performance of the contract concluded between the EU sender and the US recipient); with the second option, the data protection legislation of the Internet user country will be applicable and for instance, the US data controller will have to nominate a representative in order to comply with all Data Protection Directive requirements.

Certain authors have considered that Article 4 1 (c) must have priority insofar as it determines the scope of the application of the directive and thus the limited scope of the other provisions, namely Articles 25 and 26. We are not convinced by this reasoning. As already asserted and demonstrated by the CRID's so called study on methodology,[73] C. de Terwangne and S. Louveaux,[74] Article 4.1 (c) as a provision with extraterritorial effect must be interpreted in a narrow sense, that is to say that this provision intends to cover situations where the data controller intends to escape from the application of the European regulations by making use of 'equipment' located in a European country. That is the case notably, when the data controller is collecting data through mirror websites in the EU. That is also the case when with or without malicious intent, he collects data through the use of equipment, by placing cookies or other technical devices on the equipment of Internet users or by using technical devices placed on equipment installed in European countries (like remote sensors) which functionally are aimed at sending information to a distant place.[75] So, as regards the TBDF created by the use of the Internet, the mentioned authors have proposed to distinguish clearly the active flows and the passive flows, that means the electronic traces generated automatically from the equipment of the user by a specific device put on the equipment of the sender by the recipient and without any intervention by Internet users.

2.2. *Article 25/The General Principle and its Recent Implementation*

2.2.1. *The 'Adequate Protection' Concept*

Article 25, paragraph 1, sets out the principle that Member States[76] shall only allow a transfer to take place if a third country in question ensures an adequate level of protection.[77]

The notion of 'adequacy' has to be assessed through a case-by-case, pragmatic and functional approach.[78]

The case-by-case approach implies the study of the risks[79] directly connected with the transfer or set of transfers under consideration. Some

countries presents an adequate level of protection in certain sectors (children's privacy for instance), but not in others. Some countries may have different regulated concepts as regards 'sensitive data'.

By pragmatic approach the directive understands a 'system of rules', not only laws emanated from legislative power, but also case-law, principles of law, as well as sector rules, which can include codes of conduct, privacy policies, contractual clauses, etc.

The functional approach does not intend to find the same rules as in the European Union in a third country, but to assure that this country offers guarantees in the field of data protection in relation to the specific transfer or set of transfers under analysis. Thus, the goal is not to find the same rules, but similar rules that are considered necessary for the directive to protect properly the specific category of data.[80]

Paragraph 2 prescribes:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in a third country in question and the professional rules and security measures which are complied with in that country.

Thus, to consider 'adequate', a given level of protection is necessary to evaluate the means of expression, the means of control and the means of coercion.[81]

Means of expression are the legal tools that contain the principles of data protection. Means of control are the different methods which aim at guaranteeing the respect of principles, directly or indirectly, exclusively or not. Means of coercion are the ways and procedures of dissuasion, reparation and repression against the breach of respect to the principles of data protection.

Reference is therefore made not only to Member State laws, but also to codes of conduct provided they are complied with.[82]

Under this point, the directive is recognising the importance of self-regulation as regards countries with different legal values. This is the case, mainly, for the countries such as the US, where self-regulation is a common source of law in the privacy sphere.

In the framework of assessing third country adequacy, Article 29 Working Party issued a document entitled '*Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?*'[83] and have put certain criteria in order to assess self-regulatory instruments[84]:

I) Is the Body Responsible for the Sector?

One important criterion for judging the value of a code is the degree to which its rules can be enforced. In this context the question of whether the association or body responsible for the code represents all the operators in a sector or only a small percentage of them is probably less important than the strength of the association in terms of its ability to, for example, impose sanctions on its members for non-compliance with the code.

However, the Working Party believes that industry-wide or profession-wide codes are more useful instruments of protection than those developed by small groupings of companies within sectors for various reasons.

> First is the fact that, from the consumer's point of view, an industry that is fragmented and characterised by several rival associations, each with its own data protection code, is confusing.
>
> The second point is that, particularly in industries such as direct marketing, where personal data is routinely passed between different companies of the same sector, situations can arise where the company disclosing personal data is not subject to the same data protection code as the company that receives it. This is a source of considerable ambiguity as to the nature of the rules applicable, and it might also render investigation and resolution of complaints from individual data subjects extremely difficult.

II) Evaluating the Content of a Self-Regulatory Instrument

According to the Working group, this is a question of ensuring that the necessary 'content principles' set out in the Working document 'Transfers of personal data to third countries: applying Articles 25 and 26 of the EU Data Protection Directive'[85] are complied with (purpose limitation principle, the data quality and proportionality principle, transparency principle ...).

> It is a question of what the code contains, and not how it is developed. The fact that an industry or profession has itself played a mayor role in developing the content of the code is not in itself relevant, although clearly if the opinions of data subjects and consumer organisations have been taken into account during its development, it is more likely that the code will reflect more closely the core data protection principles which are required.
>
> The transparency of the code is a crucial element, in particular, the code should be drafted in plain language and offer concrete examples, which illustrate its provisions.
>
> Furthermore, the code should prohibit the disclosure of data to non-member companies who are not governed by the code, unless other adequate safeguards are provided.

III) Evaluating the Effectiveness of a Self-Regulatory Instrument

Assessing the effectiveness of a particular self-regulatory code or instrument requires an understanding of the ways and means by which adherence to the code is ensured and problems of non-compliance dealt with. The three functional criteria for judging the effectiveness of protection must all be met if a self-regulatory code is to be taken into consideration in the assessment of adequacy of protection.'

Good level of compliance

The level of compliance with the code is likely to depend on the degree of awareness of the code's existence and of its content among members, on the steps taken to ensure transparency of the code to consumers in order to allow the market forces to make an effective contribution, on the existence of a system of external verification (such as a requirement for an audit of compliance at regular intervals) and, perhaps most crucially, on the nature and enforcement of the sanction in cases of non-compliance.

According to the Working Party,

> when examining the types of sanction in place, it is important to distinguish between a "remedial" sanction which simply requires a data controller, in a case of non-compliance, to change its practices so as to bring them into line with the code, and a sanction which goes further by actually punishing the controller for its failure to comply. It is only this second category of "punitive" sanction which actually has an effect on the future behaviour of data controllers by providing some incentive to comply with the code on an ongoing basis. The absence of genuinely dissuasive and punitive sanctions is therefore a major weakness in a code. (...)

Support and help to individual data subjects

A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his/her personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed. This institutional support should ideally be impartial, independent and equipped with the necessary powers to investigate any complaint from a data subject.

The Working Party states some relevant questions for self-regulation in this regard such as: is there a system in place allowing for investigation of complaints from individual data subjects? How are data subjects made aware of this system and of the decisions taken in individual cases? Are there any costs involved for the data subject?

> The impartiality of the arbiter or adjudicator in any alleged breach of a code is a key point. Clearly such a person or body must be independent in relation to the data controller. However, this in itself is not sufficient to ensure impartiality. Ideally the arbiter should also come from outside the profession or sector concerned, the reason being that fellow members of a profession or sector have a clear shared of interest in the data controller alleged to have breached the code. Failing this the neutrality of the adjudicating body could be ensured by including consumer representatives (in equal numbers) alongside the industry representatives.

Appropriate redress

If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject. This remedy must put right the problem (e.g. correct or delete any inaccurate data, ensure that processing for incompatible purposes ceases) and, if damage to the data subject has resulted, allow for the payment of appropriate compensation. (...)

2.2.2. *The Commission's Decisions on Adequacy*

The general directive foresees another possibility in respect op third countries in paragraph 6, Article 25:

> The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision. In that context the Commission had to take certain decisions as regards the adequacy of regulatory systems taken or proposed by third countries.

The European Commission has adopted, up to now, three decisions under Article 25.6. The first, concerning the US and known as 'Safe Harbor',[86] determines that an arrangement put in place by the US Department of Commerce provides an adequate level of protection for personal data transferred from the EU. Decisions have been adopted concerning Switzerland[87] and Hungary.[88] In the two other cases, the US case from one side and the Hungarian and Swiss from other part are quite different: in the first case, the US Department of Commerce proposed a system grounded essentially on a self-regulatory basis; in the second case, a legislative system similar to the European one existed and both countries had adhered to the Council of Europe Convention on Data Protection. Another difference might be drawn from the fact that the US system does ensure that certain companies listed are as such offering adequate privacy protection;[89] in the case of the Hungarian and Swiss legal system, the protection was offered globally for all companies and all activities.

We will start by referring briefly to the decision concerning the US. The US point of view differs deeply from the European one insofar as privacy protection is considered as sufficiently ensured through self-regulation and not through a legislative approach considered as inadequate and costly by the US Government.

It was necessary to look for a solution to allow data flows from the EU to the US[90] within a safe framework, even more so with the increasing activities promoted by the use of the Internet. The Commission has negotiated with the US Department of Commerce for more than two years.[91] The results are the principles, which are supplemented by FAQs (Frequently Asked Questions), published by the Department of Commerce and providing guidelines for the implementation of these principles.

Adherence to these principles by US companies is voluntary.[92] When subscribing to the principles, companies must reveal their confidentiality rules and fall within the competence of the Federal Trade Commission or the US Department of Transportation.

Nevertheless, the analysis of the scope of the principles[93] leads us to conclude that there is a lack of coherence between, on the one hand, the requirement to monitor compliance with the 'Safe Harbor' principles by an institution such as the Federal Trade Commission and, on the other hand, the scope of the 'Safe Harbor'. This covers areas over which the Federal Trade Commission[94] or the US Department of Transportation[95] do not appear to have competence, such as for example telecommunications, data concerning employees, data concerning pharmaceutical details.[96]

If a transfer has to be done in one of the areas or businesses mentioned above, it will be necessary to use methodology to evaluate the level of protection given to or by this specific sector.[97] The collection of information, analysis of the risks that the flow involves and the analysis of the protection given by sector could be very expensive and complicated.

As regards the content, although there is some progress in the formulation of the principles, the absence of any precise definition of the fundamental concepts must be underlined. Thus, without claiming to be exhaustive, the concept of 'personal data' is defined vaguely by reference to the scope of the directive, but this reference does not state whether the 'Safe Harbor' principles will give the concept the same very broad scope given by Article 2.a). The concept of 'third party' itself is not defined, and does the concept of 'consent', fundamental in principle 2: 'Choice', require the same conditions as those called for by Article 3 (h) of the directive? The 'sensitive data', especially broadened in relation to the previous versions of the Safe Harbor, is defined as data 'specifying' and not, in the broad sense of the directive, as data 'revealing' racial or ethnic origin, health, sexuality, political opinions, religion, etc.[98]

As regards the effectiveness of the US self-regulatory system, certain doubts have been raised: firstly, the system lays down on the intervention of a self-

certification system where the companies themselves are assessing their own respect of the Safe Harbor principles. In the case of litigation with European citizen alleging non respect of the principles, the system provides a possible recourse before an Alternative Dispute Resolution jurisdiction (ADR) (exceptionally before the Federal Trade Commission which is an official jurisdiction very active in the data protection field). It is quite obvious that this recourse is not obvious for European citizens and that for different reasons (language spoken, reference to another legal system, ...). Furthermore, the problems of the investigation powers of this ADR and the enforcement of its decisions have been insufficiently foreseen by the Safe Harbor principles. Finally, there is a risk of no adequate sanctions except those pronounced by the FTC or other official jurisdictions.

So, as Joel Reidenberg has said,

> While the approval of the Safe Harbor was an important short-term political victory for both the US and the European Commission,[99] the Safe Harbor agreement is unworkable for both sides and will not alleviate the issues of weak American privacy protection.[100]

The Decisions concerning Switzerland and Hungary have a different approach since both countries have general data protection laws that have binding legal effect.

In the case of Switzerland, the legal standards of both Federal and cantonal level were considered (the Federal Constitution, the case-law, the Swiss data protection Act, cantonal legislation). These legal standards cover all the basic principles necessary for an adequate level of protection for natural persons. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities.

Similar considerations have been made as regards Hungary (Constitution, legal provisions, sectoral laws). Both countries have ratified the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108).

2.3. *Specific Derogations*

2.3.1. *Article 26.1. List: The Derogations as Regards Certain Types of Data Processing*

There are some cases in which a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection can take place.

They are mentioned in Article 26, paragraph 1. The list enacted again takes a certain number of legitimate purposes listed in Article 7 of the European

Directive but provides certain restrictions due to the international character of the flow and the risks linked therewith as it will be showed.

(a) The data subject has given consent unambiguously *to the proposed transfer*
Under Article 7 of the Data Protection directive, consent is the first ground to legitimate a processing within the European Union. Article 26 takes it again but impose certain restrictions: beyond the general requisites available for any consent in the sense of the directive (the consent must be freely given, specific and informed) the consent must be unambiguous and thus must explicitly refer to the international character of the flow. That implies that the data subject must be informed about the fact that data will be transferred directly or indirectly towards a third country.

In the context of the Internet the individuals are usually required to give personal data in different situations.

A European citizen, when opening a free e-mail account in a company located in the US is required to give personal data. This data will be transferred to this company which is outside the EU, with the consent of the individual. Nevertheless, sometimes this consent is not properly 'informed'. Later, this person will start receiving spam in his mailbox, or cookies on his hard disk.

(b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request
This would be frequent in the case of electronic commerce transactions. We can think about a B2C example, a person ordering goods from a company that is located outside the EU. He will give his name, address, credit card number, but as well show a consumer profile.

European national authorities can do nothing to protect this situation apart from making an education policy in order to enhance awareness of their citizens as regards the risks that exist, how to evaluate, from a consumer point of view, privacy policies of websites, or to alert from websites asking for irrelevant information.

The provision requires that the transfer must be necessary for the performance of the contract. So, the data controller located outside Europe not only has to demonstrate that the processing of the data was necessary for the performance of the contract but furthermore that the processing outside Europe was necessary. Let us take an example regarding labour contracts: a US multinational company is creating large data banks about their employees, notably European employees. This company will take benefit of the exception only if it is able to show that the transfer of data to this data bank located in the US is needed according to the specific purposes pursued by this data base. For instance, if the processing of the data is pursuing the purpose of calculating the wages of each employee, no specific need exists for centralising the data outside Europe; although if the processing concerns only certain employees

whose functions imply frequent travel and a great mobility amongst the different subsidiaries, the exception will be applicable because it will be easy to demonstrate that due to the specificity of the data transferred and the specific purposes followed by the processing, the transfer was necessary for ensuring a good performance of the labour contract concluded with this category of employee.

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party
A travel agency contracts services in the interest of its clients (hotels, flights, cars, etc.), and transfers their names, and other details, to third parties, which may be located outside the EU.

A hospital may transfer details of a patient who was assisted under the terms of a contract concluded between the hospital and the health insurance company, that may be located outside the EU.

(d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) The transfer is necessary in order to protect the vital interests of the data subject; or

(f) The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in a particular case.

These last three exceptions do not require specific comment in the context of this article insofar as they are less specific to e-commerce transactions.

2.3.2. *Contractual Clauses*

There is another alternative way[101] for making a safe transfer mainly based on self-regulation[102]: the contractual clauses.

Article 26.2 of the general directive prescribes:

> A Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedom of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

At the European level, special attention should be put on contractual solutions,[103] in view of the fact that the Commission is unlikely to adopt adequacy findings under Article 25.6 for more than a limited number of countries in short or even medium term.[104]

This possibility is also foreseen in the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) regarding supervisory authorities and transborder data flows.[105] Article 12 regulates the transborder flows of personal data to a recipient which is not subject to the jurisdiction of a party to the Convention. Contractual clauses are considered safeguards that can be taken in the case that the country of destiny does not provide an adequate level of protection, after been found adequate by the competent authorities according to domestic law.

In 1993 a study made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce was published.[106] It included an explanatory report and a model contract to ensure equivalent protection in the context of transborder data flows.

The objectives of this model contract were: (a) to provide an example of one way resolving the complex problems which arise following the transfer of personal data subjected to different protection regimes; (b) to facilitate the free circulation of personal data in the respect of privacy; (c) to allow the transfer of data in the interest of international commerce; and (d) to promote a climate of security and certainty of international transactions involving the transfer of personal data.

The model contract has 5 clauses that regulate the obligations of the licensor (data exporter), the obligations of the licensee (data importer), the liability and indemnity, the settlement of disputes, and, the termination of the contract. The scope is reduced to a 'controller to controller' situation.[107]

The parties are free to choose the law applicable to the contract between the licensor and licensee. Nevertheless, the explanatory report says that when the applicable domestic law ensures a better protection of personal data, the licensor is recommended to check whether he must complete the clauses accordingly. We have to point out that this study was made before the enactment of Directive 95/46/EC, which Article 4 regulates the applicable law in a restricted way.[108]

The clauses do not foresee a system of third party beneficiary in favour of the data subject. The licensee and the licensor are not submitted to a joint and several liability system. In fact, the licensee shall be liable for the use made of the data which has been transferred by the licensor; and, the licensee undertakes to indemnify the licensor for any breach resulting from his obligations under the contract or for any fault or manifest negligence linked to the execution of the contract.[109]

Because of the reasons briefly described above, the Commission could not accept these clause because they were not concordant with the requirements established in the Data Protection directive.

Later on, the International Chamber of Commerce updated these clauses[110] in order to meet the requirements of the Directive and to obtain a decision from the Commission based on Article 26(4).[111]

The explanatory notes describe that *'the clauses will benefit small and medium-sized enterprises in particular which may not be able easily to afford the cost of creating specific clauses themselves'*.

The ICC contract has a set of definitions and 9 clauses that regulate the warranties of the Data Exporter, undertakings of the Data Exporter and Disputes with Data Subjects or Data Protection Authorities, warranties of the Data Importer, undertakings of the Data Importer, dispute resolution, indemnities, Data Processors, and governing law.

The clauses regulate a relationship of 'controller to processor'.[112] The ICC submitted the clauses to the European Commission in 1998, the original version in September, and a revised version in December. Nevertheless,

> the Working Party analysed the ICC clauses and made further suggestions and comments. It proposed in particular that the ICC clauses should apply to controller–controller situations. This means that the clauses should provide for safeguards in the case where personal data were to be sold from the EU a new responsible abroad. Here, the individual has no protection. So far, the ICC text addresses only controller–processor situations that are, to a certain extent, covered by Article 17(3) of Directive 95/46/EC. The Working Party invited the ICC to revise its text in the light of the comments made.[113]

Returning to the Data Protection Directive, Article 26.2 provides that the appropriate contractual clauses[114] can be proposed by the controller to the Member State authority for approval and can be accepted by this authority.

Furthermore, the Commission can approve or elaborate 'Standard Contractual Clauses', as referred to in Article 26, paragraph 4:

> Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

On 15 June 2001 the Commission passed a decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC.[115]

The Decision[116] obliges Member States to recognise that companies or organisations using such standard clauses in contracts concerning personal data transfers to countries outside the EU are offering 'adequate protection'.[117] Data Protection Authorities in the Member States retain powers to prohibit or suspend data flows in exceptional circumstances, despite the use of the European Model of contractual clauses.

Use of these standard contractual clauses will be voluntary but will offer companies and organisations means of complying with their obligation to ensure 'adequate protection' for personal data transferred to countries outside the EU which have not been recognised by the Commission as providing adequate protection for such data.

The decision refers to transfers made from a 'controller'[118] who is established inside the EU to another 'controller' who is established outside the EU.

That would be the case, for instance, with regards the selling of a data base for direct marketing purposes. The buyer acquires the right to determine the purposes and means of the processing of personal data. As regards labour relationships, it is necessary to evaluate whether the Data Importer's processing is operated on behalf of the Data Exporter and under his control or might pursuit his own objectives. Let us take two examples: the first one envisages a company having its head office established in the US. The European subsidiaries will transfer employees data to the US not only for applications controlled by the sender (like payment of wages, application of social security measures) but also for internal needs of the multinational US company which will be able to answer rapidly by instance to a request of another subsidiary to constitute a research team or for seeking trainers. The processing of the data by the data bank located outside Europe is under the control of the recipient who might be qualified as a controller even if certain operations are done on behalf of the sender. In that case, the decision could be applicable. The second case is quite different: a company having its head office in Europe creates a data bank of the management personnel outside of Europe since the storage and communication costs are less expensive than in Europe. The data bank located outside Europe is totally under the control and have no possibility to develop other applications than those imposed by the European Data Controller. In that case the Importer would act 'on behalf' of the Exporter, and would be a 'processor' rather than a 'controller'. This case is not covered by the decision mentioned above.

A draft decision on Standard Contractual Clauses[119] that regulates transfers made from a 'controller' located inside the EU and a 'processor'[120] located outside the EU has been issued, in order to cover this second category of cases. It is dated 1 July 2001 and is presently subject to public comment. Certain authors and lobbies have argued that this second intervention of the Commission was not necessary[121] since the Controller exporting data to a Processor remains totally liable in case of infringements made by him and insofar as Article 17.3. of the Data Protection Directive is already providing the existence of a contract guaranteeing the protection of the data subjects. These arguments have been rejected by the European Article 29 Working Party. The fact that there is a transborder data flow creates more difficulties for the Data Subjects to be aware of illegitimate processing operated by the Data Processor and more difficulties in the case where he is entitled to obtain an appropriate redress which consist not only in penalties but also in the cessation of these illegitimate uses. For these reasons, the draft decision offers appropriate measures and is thus required.

A rapid analysis of the decision and the draft decision[122] leads to the following comments:

Clause 1 includes a set of 'Definitions'. The *decision* defines the 'Data Exporter' as the Controller who transfers personal data, and the 'Data Importer' as the Controller who agrees to receive this data for further processing; whilst the *draft* defines the 'Data Importer' as a Processor.

Clause 3 regulates a 'third party beneficiary' system. This clause entitles the Data Subject, who is not a contracting party of the contract, to enforce the clause itself (as regards the compromise of the parties who do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law) and other specified clauses of the contract as third party beneficiary.[123]

This clause is necessary to grant a contractual right to the Data Subject when his own data is involved in a contractual relationship between two other parties (he has 'interests' on the contract but he is not strictly a contracting 'party').

Otherwise, the Data Subject might not benefit of contractual provisions like the joint and several liability system, the intervention of the Data Protection Authorities, the possibility of choosing between mediation or the intervention of Member States courts if a dispute arises, etc.[124]

Nevertheless, it will be necessary to assess if the law of the country where the data exporter is located (governing law of the contract) allows or foresees the concept of 'third party beneficiary'.

This institute is quite diverse in common law[125] and continental law. For example, the Confederation of British Industry, in the Comments on the Commission's revised draft Standard Clauses,[126] refers that under UK third party rights provisions, unless specifically stated otherwise, the parties to the contract will not be able to amend or terminate it without the consent of any of the third parties involved. Precisely, the so designated Clause 9, 'Termination of the Clauses', does not mention this expressly.[127]

Clause 4 regulates the 'Obligations of the Data Exporter' as follows:

- to process the data in accordance with all the requirements and relevant provisions.
- to inform the data subjects, when the processing involves special category of data,[128] that their data could be transmitted to a country not providing adequate protection.
- to make available to the data subject upon request a copy of these clauses. This part has been seriously criticised by different organisations who addressed letters to the Commission.[129]

The *draft* regulates more obligations of the data exporter:

- to instruct the data importer to process the personal data transferred only on his behalf and in accordance with the applicable data protection law and these clauses.
- to inform the data importer of the inquiries made by Data Subjects or the Supervisory Authority concerning processing activities carried out by him.
- to inform the data importer about personal data that should be corrected, updated, deleted, blocked or whose use by determined purposes has been banned or restricted.

Clause 5 regulates the 'Obligations of the Data Importer' as follows:

- to warrant that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract.
- to process the personal data in accordance with the set of principles attached to the clauses. There are other possibilities foreseen, when agreed by the parties: a) to process the data in accordance with the relevant legislation applicable to a Data Controller in the country in which the Data Exporter is established; or b) the relevant provisions found in any Commission decision under Article 25(6) finding that a third country provides adequate protection in certain sectors of activity only, provided that the Data Importer is based in that third country and not covered by those provisions, insofar as those provisions are of a nature which makes them applicable in the sector of the transfer.

As regards the second possibility, we can assess if this would be the case of the Safe Harbor. The compliance monitoring in the US is exercised by the Federal Trade Commission and the US Department of Transportation. These institutions have no competence on areas such as telecommunications, data concerning employees, banks, etc. So, one can imagine the hypothesis of a company acting in one of these areas, which cannot adhere to the Safe Harbor itself, but can agree with the other party of the contract to process the data in accordance with the relevant provisions of the Commission decision on the adequacy of the protection provided by the Safe Harbor principles and related Frequently Asked Questions issued by the US Department of Commerce.

- to deal with all reasonable inquiries from the Data Exporter or the Data Subjects relating to the processing of the Personal Data subject to the transfer[130] and to co-operate with the competent Supervisory Authority in the course of all its inquiries.
- to submit its data processing facilities for audit.
- to make available to the Data Subjects upon request a copy of the Clauses.[131]

The *draft* regulates more obligations from the Data Importer:

- to process the Personal Data only on behalf of the Data Exporter and in accordance with his instructions and the clauses.
- to warrant that he shall use the personal data transferred solely for the provision of the data processing services on behalf of the Data Exporter and that he will not disclose the personal data transferred to third parties unless the Data Exporter has given prior written authorisation and the third party has entered into the same obligations than the data Importer; that authorisation will be incorporated and form an integral part of the contract.
- to notify the Data Exporter of any request of disclosure of the personal data transferred from a public body that could force him to disclose the data, unless such notification is forbidden by law, as well as any disclosure or accidental or unauthorised access made by an employee, subcontractor or any other identified person.
- to notify the Data Exporter of any requests received directly from the Data Subjects acknowledging that he is not authorised to respond unless the Data Exporter has explicitly authorised that action or a competent authority has declared that the Data Exporter has disappeared or for whatever reason is unable to respond to requests from the Data Subjects.
- to implement technical, organisational and security measures.

Clause 6 states the 'Liability' system. Data Subjects who have suffered damage as a result of any violation of the provisions referred to in clause 3 are entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that none of them are responsible for an act incompatible with the obligations contained in these clauses.

This first point of clause 6 is concordant with Article 23 of the Data Protection Directive:

> 1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

The Data Exporter and the Data Importer agree that they will be jointly and severally liable for damage to the Data Subjects resulting from any violation of the provisions referred to in clause 3. In the event of a violation of these obligations and/or conditions, the Data Subject can take action before a court against either the Data Exporter or the Data Importer or both.

There is an optional clause, on mutual indemnification, by which the parties can agree that if one party is held liable for a violation by the other party of any of the provisions referred to in clause 3, the second party will indemnify the first party from any cost, charge, damage, expense or loss incurred by the first party to the extent to which the second party is liable.

The ICC, in its letter[132] addressed to the Internal Market Directorate General Commissioner, dated 13 March 2001, pointed out that joint and several liability is an anomaly in commercial contracts and parties outside the EU and will be extremely reluctant to enter into clauses containing it. Despite these criticisms, the European position was not modified: the main argument seems to be the will to ensure real protection of the Data Subjects who will find suing the Exporter located in Europe before his national courts a more efficient way to get redress and damages in case of violations of the Privacy Protection requirements by hypothesis committed in a foreign country offering no adequate protection. Another argument might be found in the fact that the fear of the Exporter to be sued will create a great incentive for him to be very cautious when he exports data and to exercise real control over the activities of the importer.

Apart from these arguments, we have to bear in mind that we are dealing with a fundamental right, the right to privacy, so, commercial rules are not entirely applicable to these contract clauses.

The *draft* creates a different system, where no joint liability is foreseen:

The Data Subject is entitled to receive compensation, for the damage suffered, from the Data Exporter, either if the violation has been caused by the Data Exporter or the Data Importer.

The Data Subject can only sue the Data Importer when the Data Exporter has disappeared, filed for bankruptcy or for any other reasons a competent authority of the Data Exporter's country has determined that the Data Exporter cannot face his responsibilities and the Data Importer has violated some of his obligations under the contract.

One might observe that even if the *draft* Decision foresees more obligations for the Data Importer and the Data Exporter, they both derive from the characteristics of a subordination relationship. The different level of responsibility of each party can be easily distinguished if we compare the liability system. For the 'controller to controller' transfer, a joint and severally liability system is regulated, both parties have the same rights and duties as regards the personal data so both have the same liability. For the 'controller to processor' relationship a Data Exporter liability system is regulated, since the processor only acts 'on behalf' of the controller–exporter, the first one will be exceptionally liable in the cases already mentioned.

Clause 7 refers to 'Mediation and Jurisdiction'. The Data Subject can decide whether to enter into third party mediation or to refer the dispute to the Courts in the Member State where the Data Exporter is established.

The Data Subject can also agree with the relevant party that the resolution of a specific dispute can be referred to an arbitration body provided that that party is established in a country which has ratified the New York Convention on enforcement of arbitration awards.[133]

In these cases it will be necessary to assess whether the country where the party involved is established has ratified the Convention with the 'commercial reservation' or not.[134] This reservation means that only commercial matters can be submitted to arbitration, which is not the nature of the Data Subject's rights.

The *draft* regulates, for the situation that a dispute arise between the Data Subject and the Data Importer, that the Data Subject can submit the case to mediation or to the courts in a Member State where the Data Exporter is established.

Both the *decision* and the *draft* declare that the Data Subject can seek remedies in accordance with other provisions of national or international law.

Clause 8 foresees the 'Co-operation with Supervisory Authorities'. The parties agree to deposit a copy of the contract with the Supervisory Authority if it so requests or where deposit is required under national law.

The *draft* adds that the Supervisory Authority has the right to audit the Data Importer with the same extension and conditions the Authority would have to audit the Data Exporter under national law. This is an extraterritorial application of the powers that the National Authorities are entitled with.

Clause 10 (9 in the draft), establishes the 'Governing Law'. The clauses shall be governed by the law of the Member State where the Data Exporter is established.

This clause is concordant with Article 4 of Directive 95/46/EC, in which is stated:

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.'

Article 4 (the national regulation that transposes it) is a mandatory rule ('*loi de police*'[135] of Private International Law), by consequence, even if we are dealing with private law, the freedom of choice regulated by Article 3 of the Rome Convention on the law applicable to contractual obligations[136] is not applicable when we are dealing with personal data.

Article 7 of the Convention stipulates:

1. When applying under this Convention the law of a country, effect may be given to the mandatory rules of the law of another country with which the situation has a close connection, if and in so far as, under the law of the latter country, those rules must be applied whatever the law applicable to the contract. In considering whether to give effect to these mandatory rules, regard shall be had to their nature and purpose and to the consequences of their application or non-application. 2. Nothing in this Convention shall restrict the application of the rules of the law of the forum in a situation where they are mandatory irrespective of the law otherwise applicable to the contract.

If the contractual clauses on data protection are an annex to a main contract, this main contract can, of course, benefit from the freedom of choice as regards the applicable law. The *depeçage* is foreseen in Article 3.1, last sentence, of the Convention:

By their choice the parties can select the law applicable to the whole or a part only of the contract.

Clause 11 of the *draft* stipulates the 'Obligation after the termination of the clauses'.

At the termination of the provision of data processing services, at the choice of the Data Exporter, the Data Importer shall return all personal data transferred and its copies to the Data Exporter or shall destroy all personal data and certify to the Data Exporter that he did so, unless legislation imposed upon the Data Importer prevents him from the devolution or destruction of whole or part of the personal data transferred. In that case, the Data Importer warrants that he shall guarantee the confidentiality of the personal data transferred and shall not actively process the personal data transferred any more.

In the Appendix the parties have to specify the activities relevant to the transfer both of the Data Exporter and the Data Importer. They have to describe the categories of Data Subjects involved, the purposes of the transfer, the categories of data, the sensitive data concerned (when appropriate), the recipients to whom it is possible to disclose the data, and the storage time limit.

The Annex to the Contract 'Mandatory Data Protection Principles' is a minimum requirement of principles to be respected by the Data Importer, and has to be interpreted in the light of the provisions of Directive 95/46/EC. Nine principles[137] are mentioned as regards: purpose limitation; data quality and proportionality; transparency; security and confidentiality; rights of access, rectification, deletion and objection; restrictions on onward transfers; special categories of data; direct marketing; and automated individual decisions.

Conclusions

Contrary to the US, which consider that privacy is fundamentally a consumer concern to be put at the disposal of the Data Subject who might decide to renounce it against, for example financial incentives, EU policy does consider privacy as a fundamental right not to be subjected to the market game. Even if a certain competition exists between different companies in their offer of privacy protection, and even if this competition leads to value added systems of privacy protection, Europe does not consider that the simple Market economic regulation will offer a sufficient guarantee to the fundamental privacy requirement. In that perspective, the European texts are imposing a certain number of limitations to the companies.

So the proposed Directive severely restricts their right to process data collected through networks. It is quite obvious that the main concern of the European Union is to avoid any risk of an Orwellian society. Each of us leaves more and more evidence on the Internet which can be easier and easier collected by certain companies. The express limitations to the processing of Internet evidence are an answer to this fear of the citizens not to be able to control the circulation of their own information images in the future, and to prevent adequately their use. Particularly, the marketing use of the data collected through the Internet is severely limited and the use of the Internet for marketing purposes is also severely restricted. At the same time, following the US principle,[138] the Directive underlines the increasing role of privacy notices[139] and consent pronunciations. Personal control is, as in the US, becoming the main basis of the legitimacy of processing. The principle of notice requires the Controller to deliver fair information to the 'consumers' about how the information will be used. So informed, the 'consumer' will have the possibility to exercise his right to choose. This trend is noticeable insofar as it puts a certain responsibility on the 'consumer's' shoulders.

Member States have, under the European Model, a responsibility for preventing unbalanced situations. Despite the remarks made above, we welcome the review of Directive 97/66/EC in order to adapt it to the new technologies and to create a technology neutral framework. The Internet is not an anarchic system and the fundamental right of privacy has to be protected against any threat, and considered as a higher value than a simple business advantage. Social development cannot be measured only by economic factors since the final goal of any political effort is the individual's integrity, both physical and moral. But, there is also a place for an individual responsibility for each Internet user. The interactivity of the medium offers the increasing possibility for users to scrutinise the privacy policies proposed by the operators and to exercise control by deciding that this use is unacceptable, or, on the contrary, to deliver more personal information when, as a customer, he does want a more customised service. This presence of the US model of personal control in the recent text of the European Union must be underlined, even if this model has to be replaced in a legislative model which creates a 'higher level of privacy protection' framework. Definitively, Europeans have taken great benefit from the 'notice and choice' approach of the US doctrine.

As regards the TBDF, it is quite obvious that the 'adequate protection' principle has created a strong incentive for many countries to enact comprehensive data protection legislation. However, for pragmatic reasons, notwithstanding what certain have called the Transatlantic Privacy Dispute, the European authorities have accepted the US self-regulatory model enacted by the Safe Harbor principles[140] which have not been challenged by the Bush Administration. Even if the authors are not totally convinced by the effectiveness of the system, that remains an exception to the rule covering only 'European' data, a transatlantic consensus has been achieved and common principles have been underlined.

The contractual solutions enacted by the Commission are only beginning to take effect.[141] At first glance they bring very efficient protection to the benefit of European Data Subjects. Many provisions deeply derogate the normal contractual game. The 'privacy contract' principle is not respected and as regards the choice of applicable law, deep derogations to the autonomous choice principle have been stipulated. A lot of investigation powers have been created to the benefit of the Data Protection Authorities, and finally the several and joint liability of the Exporter and the Importer are quite derogating to commercial practices. It is too early to see how the market forces will react to these provisions but definitively the European Union has demonstrated once again the importance it gives to Privacy Protection in an Information Society.

Notes

1. Wilikens, Marc *'Information Society Technologies for Dependability and Security for Peoples'*, in *'Towards a Sustainable Information Society. Report of the Conference 21–22 February 2000'*. European Commission, Information Society Directorate-General – Unit C1. June 2000, p. 89.
2. *'Information Society Technologies. A programme of research, technology development and demonstration under the 5th Framework Programme'* 2001 Workprogramme. European Commission. Information Society Directorate-General, p. 5.
3. *'En los sistemas constitucionlaes hay una regla de oro subyacente, no necesariamente escrita pero que se infiere de la propia estructura de equilibrio que suponen los sistemas de democracia constitucional, según la cual a todo acrecentamiento del poder debe corresponder un vigorizamiento de los controles, un mejoramiento de las garantías y un acentuamiento de las responsabilidades.'* Vanossi, Jorge R. *'El Habeas data no puede ni debe contraponerse a la libertad de los medios de prensa'* El Derecho, Buenos Aires, tomo 159, p. 948.
4. *'The Internet has experienced extraordinary growth over the last years. The number of 'host' computers – those that store information and relay communications – rose from about 300 in 1981 to approximately 9 400 000 in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet in 1996 and about 200 million were expected to use it by 2000. It is expected that half of the European population will be connected to the Internet by 2005.'* Article 29 – Data Protection Working party, WP 37 *'Privacy on the Internet. An integrated EU Approach to On-line Data protection'*, available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf
5. *'Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of communication* protocols *which, more by accident than design, can lead to an invasion of the privacy of Internet users.'* While referring to the privacy risks inherent in the use of high level protocols, the document mentions some characteristics that can have serious consequences for the privacy of Internet users, namely the browser's chattering, invisible hyperlinks or cookies. Other risks can be added: data mining, spam, etc. Article 29 – Data Protection Working Party, WP 37 *'Privacy on the Internet. An integrated EU Approach to On-line Data protection'*, available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf
6. *'Many data subjects are unaware of the capacity of voyeurism that information technology has created.'* Madsen, Wayne *'Handbook of Personal Data Protection'* Macmillan Publishers Ltd., England, 1992.
7. Poullet, Yves *'Internet et vie privée: entre risques et espoirs.'* Journal des tribunaux, 17 February 2001, p. 155 and available at: http://www.larcier.be/6000.htm.
8. The US Federal Trade Commission issued a Report on Online Profiling on 13 June, 2000. There, it is explained that *'many banner ads displayed on Web pages are not selected and delivered by the Web site visited by a consumer, but by network advertising companies that manage and provide advertising for numerous unrelated Web sites. In general, these network advertising companies do not merely supply banner ads; they also gather data – in practice called online profiling which is invisible to the Web surfers. Although the information gathered by network advertisers is often anonymous, in some cases, the profiles derived from tracking consumer's activities on the Web are linked or merged with personally identifiable information. This consumer data can also be combined with data on the consumer's offline purchases, or information*

collected directly from consumers through surveys and registration forms.' The US leading Internet Network Advertisers have developed an innovative self-regulatory set of principles that addresses the privacy concerns consumers have about online profiling. The US Federal Trade Commission has applauded the Network Advertising Initiative (NAI), however, some Commissioners pointed out that legislation on the subject is still needed. See: http://www.ftc.gov/opa/2000/07/onlineprofiling.htm

9. *'In international circles, concern about the potential effect of automatic data processing upon the right to privacy began to grow during the late 1960s and early 1970s. But the eventual drafting of international measures specifically for the purpose of protecting privacy interests against the possible misuse of information by automatic means was carried out entirely by regional institutions, mostly European ones. Although the relatively rapid grow of this activity in data protection was deliberately directed at protecting one aspect of personal privacy, it is very unlikely that it would have grown so rapidly had it not been for a quite unexpected economic aspect. Some countries, especially those committed by treaty to reducing tariff barriers, began to fear that others might use their national data protection laws as non-tariff trade barriers. The development of international standards would not only establish minimum requirements for national legislation, but it could also be used to create a community of countries which met those requirements and which agreed on a free market of information among themselves, to the potential exclusion of others.'* Michael, James *'Privacy and Human Rights. An International and Comparative study, with special reference to developments in information technology'*, Ed. Datmouth. Unesco Publishing, England, 1994.
10. *O.J.* no. L 281 23/11/1995, pp. 0031–0050. Recitals 1, 3, 5, 7, 8 and 9.
11. *O.J.* no. L 024 30/01/1998, pp. 0001–0008. Recitals 1, 8 and 23.
12. There are six proposals presented by the European Commission that create a new framework for electronic communications services and networks in order to adapt Community legislation to a high-speed transformation market. The proposals are:
    - Directive on a common regulatory framework for electronic communications networks and services – sets out the horizontal provisions of the new electronic communications regulatory framework of the European Union.
    - Directive on the authorisation of electronic communications networks and services – aims at a single European market for electronic communications services by harmonising the rules for authorising provision of such services.
    - Directive on access to, and interconnection of, electronic communications networks and associated facilities – establishes a framework for access and interconnection agreements across the EU.
    - Directive on universal service and users' rights relating to electronic communications networks and services – sets out the rights that users have in respect of electronic communications services, in particular in respect of universal service.
    - Directive on the processing of personal data and the protection of privacy in the electronic communications sector – updates the current Directive to ensure it is technologically neutral and can cover new communications services.
    - Regulation on unbundled access to the local loop – introduces a requirement for local loop unbundling, designed to enter into force by 31 December 2000, in advance of the entry into force of the rest of the package.

    See COM (2000) 393, proposal for a directive of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services.
13. *'The regulatory framework that defines the environment in which companies conduct business has evolved over decades and centuries. It is adjusted to the needs of the 'old economy'. No wonder then that the Internet economy, characterised by no frontiers, intangibility and – to a certain degree – anonymity, requires adaptations of existing laws, rules and regulations. Because of the speed of the Internet development, the adaptation process in many cases lags behind, resulting in legal uncertainty.'* in *'Benchmarking Telework and E-commerce in Europe. ECATT Final Report.'* European Commission. IST programme. KAII: New Methods of Work and Electronic Commerce. August 2000, p. 157.
14. *'The Internet and privacy: What regulation?'* Notes for the closing address by Commissioner Mario Monti, Rome, 9 May 1998, available at: http://www.europa.int/comm/internal_market/en/speeches/rome0598.htm.
15. See on that point, the opinion issued by the Economic and Social Committee of the European Union (Session 24–25 January 2001, published at *O.J.* 25.4.01, C 123/1).
16. See, notably the results of these surveys analysed by the Alvergnat's Report presented before the French Data Protection Authority (the CNIL) and adopted by it on 14 October 1999 (report available at the CNIL's website: http://www.cnil.fr.) demonstrating that privacy is considered definitively as the major concern for US Internet users as regards their use of the Internet.
17. COM (2000) 385, 12/07/2000. *O.J.* 19/12/2000. Hereinafter 'the Proposal'.
18. We will come back to this issue while referring to 'unsolicited communications'.
19. About Echelon, the global surveillance system of satellite communications and the European debate thereabout, see the draft report submitted by G. Schmidt before the Temporary Committee on the Echelon Interception System, European Parliament, 18 May 2001 (PR/439868EN.doc) ; J-M. Dinant, Y. Poullet, Le réseau Echelon: Existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger?, available at the CRID's website: http://www.droit.fundp.ac.be/crid.htm. More recently, D. Yernault, De la fiction à la réalité: Le programme d'espionnage électronique global 'Echelon' et la responsabilité international des Etats au regard de la Convention européenne des droits de l'Homme, *R.I.D.A.*, 2000/1, 136, and ff..
20. *'The 1999 Communications Review'*, European Commission, DG INFSO, Directorate A. September 2000.
21. Directive 97/66/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, *O.J.*, L 24, 30.1.1998, p. 1.
22. §3 of the recitals of the Proposal.
23. This question has been discussed, but now the doctrine is unanimous to apply Directive 97/66/EC to the Internet services even if it was not the main purpose of the Directive when it was written. The Directive on certain legal aspects of the electronic commerce (enacted on 8 June 2000, *O.J.* 17.7.00) explicitly recognises the applicability of Directive 97/66/EC on the Information Society Services since its preamble and its provisions are referring to this Directive.
24. Proposal for a Directive of the European Parliament and of the Council establishing a common framework for electronic communications services and networks, COM (2000) 393 final – 2000/0184 (COD), *O.J.*, 19.12.2000, C 365 E/198.
25. Article 2.(b).
26. Why not have taken again the definition of Information Society services given by the Directive on regulatory transparency (Directive (98/48/EC) of 20 July 1998) : *'any service normally provided against remuneration, at a distance, by electronic means ...'*?
27. This interpretation of the terms of the directive is in line with the position of the European Court of Justice which maintains that remuneration does not necessarily need to be paid by the recipient of the service. Case C – 109/92, Wirth (1993), ECR I-6447, 15.
28. Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the

protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp36en.pdf.

29. See in particular Articles 12 to 15 of Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *O.J.* 17.7.2000, L 178/1.
30. The Directive 97/66/EC mentions 'telecommunications services', expression that has been changed in order to favour the concept of neutral technology.
31. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
32. Article 1.2 of the Proposal. Directive 97/66/EC protects both physical and legal persons. The Proposal mentions 'the protection of legitimate interests'.
33. *'This provision is especially relevant for the providers of* routers *and connecting lines as these facilitates carry massive amounts of information.'* Article 29—Data Protection Working Party, WP 37 'Privacy on the Internet. An integrated EU Approach to On-line Data Protection', available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf. A *'router'* is defined in the glossary of this document as *'an important devise, which provides routes for* TCP/IP networks. *This means that TCP/IP route is dynamic, depending on the failure or overloading of some routers or links. It can also be used as a* firewall *between an organisation and the Internet and guarantees that only authorised IP addresses can originate from a particular* ISP.*'*
34. *'The Role of Technology in Facilitating On-line Privacy'*, Results and Conclusions of a Workshop for Identifying Technology Requirements to Support EU Data Protection Legislation. European Commission. Joint Research Centre. Institute for Systems, Informatics and Safety. Brussels, 17 May 2000.
35. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.pdf
36. This principle is unchanged except for the replacement of 'telecommunications services' by 'electronic communications service'.
37. *'Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States'*, Recital 2 of the Proposal.
38. *'In principle, this Article refers to the content of the communications. The distinction between traffic data and data is not, however, easy to apply in the context of the Internet, and certainly not when referring to surfing. Surfing data could in principle be regarded as traffic data. However, the Working Party thinks that surfing through different sites should be seen as a form of communication and as such should be covered by the scope of Article 5.'* Article 29—Data Protection Working Party, WP 37 *'Privacy on the Internet. An integrated EU Approach to On-line Data Protection.'*, available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf.
39. Article 5 §2 of the Proposal.
40. Article 2(a) of the Proposal.
41. It must be reminded here that the Proposal does not apply to closed networks such as an intranet in a company. However this provision will apply to any use by an employee within the workplace of a public communications network.
42. Article 15.1 of the Proposal.
43. See Article 8.2 of the European Convention of Human Rights.
44. http://conventions.coe.int/treaty/en/projets/FinalCybercrime.htm.

45. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
46. Article 29—Data Protection Working Party, WP 37 'Privacy on the Internet. An integrated EU Approach to On-line Data Protection.', available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf. The European Parliament Committee in charge of the analysis of the proposed Directive has considered that cookies, hidden identifiers or similar devices that enter user's equipment are also traffic data and their processing must therefore require the user's consent.
47. Article 29—Data Protection Working Party, WP 37 *'Privacy on the Internet. An integrated EU Approach to On-line Data Protection'*, available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf. The Committee of the European Parliament has considered that the definition of data must be extended in order to cover data which are processed for the purpose of billing a communication. Furthermore, it has proposed the extension to the data, which are necessary for billing purposes not only as regards the subscribers but also intermediaries.
48. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
49. http://conventions.coe.int/treaty/en/projets/FinalCybercrime.htm.
50. *'The location of installed devices such as fixed ATMs and EFT/POS terminals (e.g. those in taxis), and of small modems, codecs and Ethernet and other network interfacing cards, are all much more ambiguous. Devices such as cellular phones, and portable and hand-held computers, are by definition mobile, and additional information is needed in order to draw inferences about their location at the time of a particular event.'* Clarke, Roger *'Person-location and person-tracking : technologies, risks and policy implications'*, 21st International Conference on Privacy and Personal Data Protection. Comissão Nacional de Proteção de dados. Portugal. Available at www.pco.org.hk/download_doc/clark-paper1.doc.
51. Poullet, Yves, *'Internet et vie privée : entre risques et espoirs.'* Jounal des tribunaux, 17 February 2001, p. 155 and available at: http://www.larcier.be/6000.htm.
52. *'Location technologies provide, to parties that have access to the data, the power to make decisions about the person subject to the surveillance, and to take action for or against their interests. These actions may be based on the place where the person is, or a place where the person is not, or has not been. Tracking technologies extend that power to a succession of places a person has been, and also a place that they appear to be going.'* Clarke, Roger *'Person-location and person-tracking: technologies, risks and policy implications'*, 21st International Conference on Privacy and Personal Data Protection. Comissão Nacional de Proteção de dados. Portugal. Available at www.pco.org.hk/download_doc/clark-paper1.doc.
53. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
54. Article 12 only applies to natural persons (§3). However Member States shall also ensure that the legitimate interests of subscribers other than natural persons are protected as concerns their entry into public directories.
55. Does this mean that subscribers can decide which data can be included or not? Under the opinion of the Committee, only those personal data strictly necessary to identify a particular subscriber would be included in public directories, except if the subscriber agreed to provide additional data.The question still remains: which are the data strictly necessary for the identification of a subscriber?

56. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
57. Article 12.
58. *'Electronic mailing and data protection'*, Commission Nationale de l'Informatique et des Libertés, France, 14 October 1999.
59. Article 29 – Data Protection Working Party, WP 37 *'Privacy on the Internet. An integrated EU Approach to On-line Data protection'*, available at http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp37en.pdf.
60. This provision will cover also SMS messages, sound-attachments, pictures and digital movies.
61. Article 13.1 of the Proposal.
62. Recommendation no. (85) 20 of Committee of Ministers to Member States on the protection of personal data used for the purposes of direct marketing, adopted 25 October 1985.
63. Germany, Austria, Italy, Finland and Denmark.
64. Opinion 7/2000 of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, *op. cit.*
65. This can be referred to as 'double opt-in'.
66. The E-commerce Directive requires that a minimum set of informations have to be fullfilled by commercial communications to ensure consumers' confidence and fair-trading, notably a clear identification of the nature of the message as commercial communication.
67. This consent could be withdrawn at any time.
68. Th. Léonard, Y. Poullet, *'Les libertés comme fondement de la protection des données nominatives'*, in F. Rigaux, *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, no. 17, Bruxelles, Larcier, 1992.
69. E.g. pop-up screens with advertising, screens suggesting to downloading images, software or other concepts, invitation to hyperlinked web site, etc.
70. Recently, on that issue, see the article written by B. Havelange, A.C. Lacoste, Les flux transfrontières de données: analyse de questions pratiques. *J.T.D.E.*, 2001, to be published.
71. As regards the EC national law applicable, see Article 4.1 and 2. For a comment on these provisions, see the article of L. Bygraeve, *'Determining applicable law pursuant to European data protection legislation'*, in E-Commerce law and practise in Europe. Edited by I. Walden and J. Hornle under the auspices of the ECLIP Network. Woodhead Publishing Limited. Cambridge, England, 2001, Chap.I/section 5/I and the numerous articles quoted by the author.
72. When at the automatic request of a foreign company, request ensured by a software programme giving instructions at regular periods (each day, for instance), European company transfers from its data base a certain number of informations, the foreign company is, in the broad sense of the expression, 'making use of the equipment' of the data sender insofar as the sender's information system is programmed in order to answer automatically to the request of the recipient's information system.
73. Y. Poullet, B.Havelange, *'Methodology for evaluating the adequacy of the level of protection of physical persons with respect to personal data processing. Executive Summary'*, published by the European Office of Publication, 1997 (Contract ETD/95/B5-3000/165). The entire study: Poullet, Yves; Havelange, Bénédicte; Boulanger, Marie-Hélène; Lefebvre, Axel *'Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel.'* Rapport Final, Centre de Recherches Informatique et Droit, University of Namur, Belgium. European Commission, DG XV. December 1996. Available on the CRID's website: http://www.droit.fundp.ac.be/crid.htm.
74. C. de Terwangne and S. Louveaux, Data Protection and online networks, Computer Law and Security Report, 234–238. Recently, L. Bygraeve has approved the reasoning held by the Namur team (see, *op. cit*)
75. On that point, see Havelange – Lacoste, *op. cit.*
76. Member States have also dealt with this problem within their own systems. For example, the Spanish Authority, *Agencia de Protección de Datos*, has passed the *Instrucción 1/2000 de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos*. Available at: http://www.agenciaprotecciondatos.org/datd10.htm.
77. At national level, it would be interesting to consider the Spanish case before the transposition of Directive 95/46/EC, where some *'Órdenes'* have been passed in order to mention the countries which have an 'equivalent' legislation to the Spanish one (we see that the regulations mention the word 'equivalent' instead of 'adequate' because, as we have already referred, they have been passed before the transposition) The *'Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección equivalente a la española, a efectos de transferencia internacional de datos' (BOE n. 35, de 10 de febrero de 1995)*, prescribe that these countries are: *'Alemania, Austria, Dinamarca –con la excepción del territorio de las Islas Feroe y Groenlandia–, Eslovenia, Finlandia, Francia, Irlanda, Islandia, Luxemburgo, Noruega – con la excepción del territorio de Svalbard – Países Bajos, Portugal, Reino Unido – inclusive el territorio de las Islas de Man y Jersey – y Suecia.'* Including as well : *'Australia, Israel, Hungría, Nueva Zelanda, República Checa, República de Slovakia, San Marino y Suiza.'* It is also mentioned which countries offer an equivalent level of protection as regards public records : *'Andorra y Japón.'* As regards *Canadá* a distinction is made between public data bases, which are protected in this country, and private data bases, recognising that only the following provinces give equivalent protection : *'las provincias canadienses de Quebec, Ontario, Saskatchewan y Columbia Británica.'* There is a second regulation: *'Orden de 31 de julio de 1998 por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos' (BOE n. 200, de 21 de agosto de 1998)*, extending the relation to Italy and Greece.
78. Poullet, Yves, Bénédicte Havelange, Marie Hélène Boulanger, Axel Lefebvre, *'Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel.'* Rapport Final, Centre de Recherches Informatique et Droit, University of Namur, Belgium. European Commission, DG XV. December 1996.
79. *'Le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage. Dans le cas de transferts de données personnelles, nous avons classifié les risques en quatre grandes catégories, que nous détaillons ci-dessus: ce sont les risques de perte de contrôle, de réutilisation des données, de manque de proportionnalité et d'inexactitude de ces données.'* Poullet, Havelange, Boulanger et Lefebvre, *op. cit.*
80. *'L'objectif de la directive n'est en effet pas d'exporter son modèle réglementaire hors de ses frontières; son but, au contraire, est de protéger les données des personnes bénéficiant au départ de la protection de la directive, y compris lorsque celles-ci sont envoyées à l'étranger.'* Poullet, Havelange, Boulanger and Lefebvre, *op. cit.*
81. Poullet, Havelange, Boulanger and Lefebvre, *op. cit.*
82. An official document was published as regards electronic commerce during the Clinton administration, where it is considered that *'governments must adopt a non-regulatory,*

market-oriented approach to electronic commerce'. The paper suggests a set of principles to consider in the field: *'1) The private sector should lead; 2) Governments should avoid undue restrictions on electronic commerce; 3) Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce; 4) Governments should recognize the unique qualities of the Internet; and, 5) Electronic commerce over the Internet should be facilitated on a global basis'*. When dealing with specific issues, the document says concerning privacy: *'The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution'*. The White House, July 1, 1997, *'A Framework for Global Electronic Commerce'*, available at: http://www.ecommerce.gov/framework.htm.

83. Adopted on 14 January 1998, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.
84. See the above mentioned document for the complete elaboration of the opinion made by the Working Party.
85. Adopted on 24 July 1998, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.
86. Commission Decision pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/decision.pdf.
87. Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Switzerland. *O.J.E.C.* L 215, 25/08/2000.
88. Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Hungary. *O.J.E.C.* L 215, 25/08/2000
89. In our opinion, a company who has subscribed to the Safe Harbor is not entitled to restrict this statement to certain activities (except as regards certain data or processing which have been excluded by the Safe Harbor Principles themselves like employment data) or by excluding the enforceability of their statement for certain countries or services, to provide an appropriate protection by other means, like by contractual means. In our opinion, such an attitude would be against the principle of the Safe Harbor statement which is clearly an assertion of the respect of privacy standards for all the activities of the US company and could therefore be considered as a false or deceptive statement.
90. Recital 4 of the Commission Decision says: *'Given the different approaches to data protection in third countries, the adequacy assessment should be carried out and any decision based on Article 25(6) of Directive 95/46/EC should be enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments.'*
91. Article 29 Working Party have been very active delivering opinions on the level of protection provided by the 'Safe Harbor' principles. These include:
WP 15: Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States.
WP 19: Opinion 2/99 on the Adequacy of the 'International Safe Harbor Principles' issued by the US Department of Commerce on 19 April 1999.

WP 21: Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed 'Safe Harbor Principles' on the adequacy of the 'International Safe Harbor principles'.
WP23: Opinion on Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the 'international Safe Harbor principles'.
WP 27: Opinion 7/99 on the Level of Data Protection provided by the 'Safe Harbor' principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 & 16 November 1999 by the US Department of Commerce.
WP 31: Opinion 3/2000 on the EU/US dialogue concerning the 'Safe Harbor' arrangement.
WP 32: Opinion 4/2000 on the level of protection provided by the 'Safe Harbor principles'.

92. The US Department of Commerce publishes a list with the organizations that have notified their adherence to the Safe Harbor framework. When consulted on 20/08/01, the list included 30 organizations. It can be checked at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
93. For a deeper analysis on the principles and FAQs consult: Poullet, Yves *'The "Safe Harbor Principles": An Adequate Protection?'* International Colloquium organised by IFCLA. Paris, 15–16 June 2000, available at http://www.droit.fundp.ac.be/crid.htm.
94. *'The jurisdiction of the Federal Trade Commission under Section 5 is excluded with respect to: banks, saving, loans and credit unions; telecommunications and interstate transportation common carriers, air carriers and packers and stockyard operators. Although the insurance industry is not specifically included in the list of exceptions in Section 5, the McCarran-Ferguson Act leaves the regulation of the business of insurance to the individual states. However, the provisions of the FTC Act apply to the insurance industry to the extent that such business is not regulated by State law. The FTC retains residual authority over unfair or deceptive practices by insurance companies when they are not engaged in the business of insurance.'* Extracted from Annex VII to the Commission Decision of pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy principles and related Frequently Asked Questions issued by the US Department of Commerce. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/decision.pdf.
95. *'The US Department of Transportation acts on the basis of its authority under Title 49 United States Code Section 41712. The US Department of Transportation institutes cases based on its own investigations as well as formal and informal complaints received from individuals, travel agents, airlines, US and foreign government agencies.'* Extracted from Annex VII to the Commission Decision of pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/decision.pdf.
96. Poullet, Yves *'The "Safe Harbor principles": An Adequate Protection?'* International Colloquium organised by IFCLA. Paris, 15–16 June 2000, available at the CRID's website: http://www.droit.fundp.ac.be/crid.htm.
97. Poullet, Havelange, Boulanger and Lefebvre, *op. cit.* The authors develop the steps towards a methodology of analysis.
98. Poullet, Yves *'The "Safe Harbor principles": An Adequate Protection?' op. cit.*
99. See on that point the interesting comments proposed by Carter H. Manny, *'European and American Privacy: Commerce, Rights and Justice'*, to be published in the Proceedings of the Academy for Legal Studies in Business Conference, held at Albuquerque, New Mexico, Aug. 2001: *'When European state that privacy is a fundamental human right, the effect among American is to frame questions of consumer information privacy in*

terms of privacy interests of individuals competing against organizational or social interests. When privacy is characterised as a right to control one's personal information or as a right of non intrusion, the American response is to allow many organizations to dominate the privacy adjustment process by setting the default at zero privacy. This means that each individual consumer has the burden of learning about the default setting and following the procedures set by organizations to elect a higher level of privacy. It is up to the individual to assert these rights. In Europe, the rights approach to privacy is quite different. Privacy rights are protected by government which has set a high level of privacy protection as a default. The burden of changing the default is placed on the business, who must convince the consumer to consent to a lower level of privacy protection. Thus, the characterisation of privacy as a right leads to very different approaches to privacy in the US and Europe.'

100. *'US Safe Harbour Principles Come Under Fire.'* (8 March 2001, the US Subcommittee on Commerce, Trade, and Consumer Protection heard several witnesses on the implications of the EU Data Protection Directive for US privacy policies. Among the witnesses were Professor Stefano Rodota, Italy's Data Protection Commissioner and Chairman of the EU Data Protection Working Party, David Smith, Assistant Commissioner, Office of the UK Information Commissioner, and Professor Joel Reidenberg, Professor of Law, Fordham University, Faculty of Law, New York.) Privacy Laws & Business, Issue no. 58, May 2001, p. 14–16.
101. *'The interest in privacy contracts is timely given the growing complexity and dynamic nature of the global information economy and information society. This interest should not be dismissed as mere politics, or as a means of gracefully acknowledging the different philosophical approaches to achieving privacy protection between jurisdictions. The issue of personal privacy requires a multilateral approach using a variety of mechanisms tailored to the particular environments in which they must operate.'* Longworth, Elizabeth *'Contractual Privacy Solutions.'* 22nd International Conference on Privacy and Data Protection, Venice, 27–30 September, 2000.
102. *'Contracts are, as such, a way for contracting parties to self-regulate their relationships. It might also be a way for one of the party to enforce vis à vis the other one a self-regulatory solution.'* Poullet, Yves *'How to regulate the Internet: New Paradigms for the Internet Governance.'* E-Commerce law and practise in Europe. Edited by I. Walden and J. Hörnle under the auspices of the ECLIP Network. Woodhead Publishing Limited. Cambridge, England, 2001.
103. Historically, the contractual model has been used for the first time in the Citibank case. The German subsidiary of Citibank entered into a contract with the German Railway Company in order to offer the customers of this company the possibility to use a credit card. The Berliner Data Protection Authority imposed the conclusion of a specific contract on privacy issue to Citibank since this company would transfer the railway card information to the US. On that issue, see A. Dix, *'The German railway card: A model contractual solution of the 'adequate level of protection' issue'*, available at: http://www.datenschutz-berlin.de/doc/int/konf/18/bahn_en.htm.
104. Recital 5, Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC.
105. Available at http://conventions.coe.int/Treaties/Html/179.htm.
106. Available at : http://www.legal.coe.int/dataprotection/Default.asp?fd=pub&fn=CtypeE.htm.
107. 'The clauses of the model contract have been designed to allow the transfer of personal data between independent economic entities.' Model contract to ensure equivalent protection in the context of transborder data flows with explanatory report. Available at: http://www.legal.coe.int/dataprotection/Default.asp ?fd=pub&fn=CtypeE.htm

108. We will come back to the topic 'Applicable law'.
109. Clause number 3.
110. Model clauses for use in contracts involving transborder data flows. International Chamber of Commerce. 23 September 1998. Available at : http://www.iccwbo.org/home/statements_rules/rules/1998/model_clauses.asp
111. See below.
112. *'They are drafted for use in two-party transactions. This might occur, for example, between a commercial entity and a data processing service provider in another country or between two members of the same group of companies sharing human resources or other personally identifiable information.'* Model clauses for use in contracts involving transborder data flows. International Chamber of Commerce. 23 September 1998. Available at : http://www.iccwbo.org/home/statements_rules/rules/1998/model_clauses.asp.
113. Article 29 – Data Protection Working Party. *'Fourth Annual Report on the Situation Regarding the Protection of Individuals with regard to the Processing of Personal Data and Privacy in the Community and in Third Countries.'* Adopted on 17.05.2001. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp46en.pdf.
114. *'La primera vez que se ha utilizado la solución contractual* (in Spain) *en el contexto de la Transferencia Internacional ha sido a finales de 1998. Las claúsulas que se han exigido han sido las siguientes: a) Obligación a las partes de la Transferencia a garantizar que se aplican íntegramente el conjunto de principios de protección de datos; b) Delimitación de la finalidad del tratamiento. Garantía de que los datos de carácter personal no podrán utilizarse para fines distintos de los especificados en el contrato y de que no pueden ser cedidos a terceros en el país de destino de la transferencia, ni siquiera para su conservación, siendo necesaria su destrucción o devolución al responsable una vez cumplida la prestación contractual; c) Calidad y proporcionalidad de los datos; d) Delimitación del interés legítimo del responsable del tratamiento, garantizando que este interés no va en detrimento de los derechos del afectado y que no se ha procedido a informar al titular del hecho de la Transferencia Internacional debido a que no existe ningún riesgo de atentado contra la intimidad, y que requeriría un esfuerzo desproporcionado informar al afectado del hecho de la transferencia.'* Agencia de Protección de Datos (Spain) *'Memoria 1998'*. Madrid, 1999, pp. 110–111.
115. Available at http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf.
116. As regards the decision the preliminary draft issued in September 2000 was more extensive and detailed. It had five appendixes related to specific cases, as follows: 1) transfer of personal data for management of labour relationships; 2) transfers for general business and administrative purposes; 3) transfer of personal data for banking, credit, insurance, fund management, tourism and transportation purposes and other business using a network; 4) transfers for marketing purposes; and 5) transfers for scientific research purposes. Each appendix required specific information as regards the data exporter, data importer, data subjects, purposes of the transfer, classes of data transferred, sensitive data, and supplementary warranties.
117. When this decision was in the process of approval, the European Commission received several letters from interested parties showing their concern, critics, etc, as regards the draft (e.g. from the US Securities Industry Association, the International Chamber of Commerce, the Confederation of British Industry, the EU Committee of the American Chamber of Commerce in Belgium, the US Department of the Treasury). These letters and the answers sent by the European Commission are available at http://europa.eu.int/comm/internal_market/en/dataprot/news/clausesexchange.htm The Commission has also published a set of Frequently Asked Questions in order to summarise the main

issues of the decision and to provide information to individuals and companies. Notwithstanding, *'they are not part of the Commission decision, have not gone through a consultative process either with the Article 29 Working Party or the Management Committee and do not have a legal status of their own.'* See: http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clausesfaq.htm.

118. '"controller" *shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.'* Article 2, paragraph d, Directive 95/46/EC
119. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/sccprocessors.htm.
120. '"processor" *shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'*. Article 2, paragraph e, Directive 95/46/EC.
121. One might also consider the first reaction of the Article 29 Working Party to the model clauses submited by the ICC : *'So far, the ICC text addresses only controller–processor situations that are, to a certain extent, covered by Article 17(3) of Directive 95/46/EC.'* (the underlined 'to a certain extent' was made by us) Article 29 – Data Protection Working Party. *'Fourth Annual Report on the Situation Regarding the Protection of Individuals with regard to the Processing of Personal Data and Privacy in the Community and in Third Countries.'* adopted on 17.05.2001. available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp46en.pdf.
122. We will describe the relevant clauses of the decision, and then, if it is appropriate, we will point out the differences with the draft.
123. *'The clause conferring rights on a third party is a promise given by one of the parties to a contract, generally in exchange for an undertaking given by the other party, to provide a benefit to a third party. This mechanism is, for example, used in insurance: insurance taken out by the controller (covering goods being transported, which could be sold over and over again during that time: the benefit of the insurance will fall to the person who owns the goods at the time of the insured incident), life insurance (for the benefit of the surviving spouse, born or unborn children)...'* Report by Huet, Jerôme *'Study contracts involving the transfer of personal data between parties to Convention Ets 108 and third countries not providing an adequate level of protection'*. Council of Europe, January 2001. Available at: http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapHuetE.htm.
124. Apart from Clause 3 itself, Data Subjects can enforce Clause 4 (b), (c) and (d), Clause 5 (a), (b), (c) a,d (e), Clause 6 (1) and (2), Clause 7, 9 and 11 as third-party beneficiaries.
125. In English law, '*although it has now been recognised, under the Contracts (rights of third parties) Act of 1999, some fairly strict conditions are laid down. In particular, under section 1, sub-section 3 of the Act, the third party covered by the clause must be expressly identified, or must be a 'member of a class' or 'answer a particular description'. It will be worth seeing whether the English courts consider the subjects of automatic processing of personal data by a corporate body, which can involve data of an extremely diverse nature, constitute members of a class or answer a particular description.'125* Report by Huet, Jerôme *'Study contracts involving the transfer of personal data between Parties to Convention n° 108 and third countries not providing an adequate level of protection*
126. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses-exchange.htm.

127. On the contrary, according to English Common Law requirement, Clause 11, 'Variation of the Contract', states that the parties agree not to vary or modify the terms of the clauses. Other problems linked with the third beneficiary principle might be quoted: What happens if the contract is void? To what extent does the Data subject invoke a right on the basis of a void contract by instance declared as such precisely because certain provisions have been considered as illegal insofar that these provisions were judged against privacy protection mandatory rules.
128. This is sensitive data, data relating to offences, criminal convictions or security measures.
129. However, the Commission has published a first set of Frequently Asked Questions when the Decision was in the process of approval, stating in FAQ no. 7 that *'in the case of the standard contractual clauses, the clauses relating to the individual's data are those already in the public domain, and published in annex to the decision. All other clauses relating to the company's business can remain confidential. Moreover, data protection authorities and the European Commission are bound by a duty of confidentiality when exercising their duties.'* Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/clausesfaq.htm.
130. The *draft* does not mention the obligation of the Importer to deal with the inquiries made by the data Subjects. The Data Importer, as Processor, is just acting 'on behalf' of the Data Exporter, he is not directly responsible, he is just doing what the Exporter wants him to do, and if not, the Exporter will be responsible for this breach.
131. The *draft* points out that the Data Importer will have this obligation only in the cases where the Data Subject is unable to obtain a copy from the Data Exporter.
132. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses-exchange.htm.
133. Available at : http://www.uncitral.org/english/texts/arbitration/NY-conv.htm.
134. All the Member States have ratified the Convention,. Two Member States (Denmark and Greece) have made the following reservation : 'State will apply the Convention only to differences arising out of legal relationships whether contractual or not which are considered as commercial under the national law.' See : United Nations Commission on International Trade Law (UNCITRAL). Status of Conventions and Model Laws. (checked on 27/08/08). Available at : http://www.uncitral.org/english/status/status-e.htm.
135. *'La catégorie des 'lois de police' est précisemént l'une de celles qui conduisent à déterminer le domaine territorial de la loi plutôt qu'à rechercher la loi applicable à une situation typique.'* Rigaux, François *'La loi applicable à la protection des individus à l'egard du traitment automatisé des données à caractère personnel.'* Revue Critique de droit international privé. Paris, 1980, pp. 443–478.
136. *O.J.* C 027, 26/01/1998, p. 0034–0046, consolidated version. Hereinafter 'the Convention'.
137. This list of principles is a strict copy of the criteria laid down by the Working Document: *'Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries'*.Available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp9en.pdf.
138. *'The idea of personal control is embodied in one of the earliest efforts to draft standards for information privacy: the Fair Information Practices formulated by the US Department of Health, Education and Welfare in 1973. Personal control is the basis for the concepts of notice and choice which played an important role in US thinking about privacy.'* (Carter H. Mammy, *'European and American Privacy: Commerce, Rights and Justice', op. cit.*).
139. In the same line, please note that the Working Party on the protection of individuals with regard to the processing of personal data has issued a Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European

Union providing concrete indications on how the rules set out in the data protection directives should be applied to the most common processing tasks carried out via the Internet. The recommendations are set out as a minimum set of obligations which must be followed by controllers operating web sites. Amongst these recommendations, the Working Party sets out a series of information to be provided to the data subject. This information can therefore be considered as a set of minimal information to be found in a Privacy Statement. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp43en.pdf.

140. It is apparent that the legislative approach followed in Europe could be explained by historic and cultural factors after the Second World War where fascist governments used personal data for identifying and imprisoning millions and millions of Jews.

141. The decision took effect on 3 September 2001.